Andrew G. Gunem (SBN 354042)
agunem@straussborrelli.com
STRAUSS BORRELLI PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, IL 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109

Attorneys for Plaintiff and Proposed Class

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF CALIFORNIA

ELLEN PACE on behalf of herself and all others similarly situated,

Plaintiff,

v.

OMNI FAMILY HEALTH,

Defendant.

Case No. 1:24-at-00857

CLASS ACTION COMPLAINT
FOR DAMAGES, INJUNCTIVE RELIEF, AND EQUITABLE RELIEF FOR:

1. **NEGLIGENCE;**
2. **NEGLIGENCE *PER SE*;**
3. **BREACH OF IMPLIED CONTRACT**
4. **BREACH OF THE IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING**
5. **UNJUST ENRICHMENT**
6. **INVASION OF PRIVACY**
7. **VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW**
8. **VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT**
9. **VIOLATION OF THE CALIFORNIA CUSTOMER RECORDS ACT**
10. **VIOLATION OF THE CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT**
11. **DECLARATORY JUDGMENT**

DEMAND FOR JURY TRIAL

Plaintiff, Ellen Pace ("Plaintiff"), on behalf of herself and all others similarly situated, states as follows for her class action complaint against Defendant, Omni Family Health ("Omni" or "Defendant"):

INTRODUCTION

1. This Class Action arises from a recent cyberattack resulting in a data breach of sensitive information in the possession and custody and/or control of Defendant (the "Data Breach").

2. On information and belief, the Data Breach was discovered by Defendant on August 7, 2024, when Defendant was alerted to cybercriminals having posted patients' most sensitive information on the dark web. Following an internal investigation, Defendant learned the Data Breach resulted in unauthorized disclosure, exfiltration, and theft of current and former patients' highly personal information, including first and last names, Social Security number, date of birth, health insurance information, ("personally identifying information" or "PII"), and medical information ("protected health information" or "PHI"). Plaintiff refers to both PII and PHI collectively as "Sensitive Information."

3. On or around October 10, 2024–two months after the Sensitive Information from the Data Breach was said to be posted on the dark web– Omni finally began notifying some Class Members about the Data Breach ("Breach Notice"). The Breach Notice is attached as Exhibit A. However, upon information and belief, notice is ongoing, with some Class Members, including Plaintiff still awaiting their formal Breach Notice.

4. Due to intentionally obfuscating language, it is unclear when the Breach actually took place and how long cybercriminals had unfettered access to Plaintiff's and the Class's most sensitive information.

5. Omni took at least two months before informing some Class Members even though Plaintiff and thousands of Class Members had their most sensitive personal information accessed, exfiltrated, and stolen, causing them to suffer ascertainable losses in the form of the loss of the

benefit of their bargain and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

6. Omni's Breach Notice obfuscated the nature of the breach and the threat it posted—refusing to tell its patients when the Breach occurred, how many people were impacted, how the breach happened, and why it took Defendant until October 2024 to begin notifying victims that hackers had gained access to highly private Sensitive Information.

7. Defendant's failure to timely detect and report the Data Breach made its patients vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their Sensitive Information.

8. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII and PHI misuse.

9. In failing to adequately protect Plaintiff's and the Class's Sensitive Information, failing to adequately notify them about the breach, and by obfuscating the nature of the breach, Defendant violated state and federal law and harmed an unknown number of its current and former patients.

10. Plaintiff and members of the proposed Class are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiff and members of the proposed Class trusted Defendant with their Sensitive Information. But Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

11. Plaintiff is a patient and Data Breach victim.

12. Accordingly, Plaintiff, on behalf of herself and a class of similarly situated individuals, brings this lawsuit seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in Defendant's possession.

PARTIES

13. Plaintiff, Ellen Pace is a natural person and citizen of California, where she intends to remain. Plaintiff received Omni Breach notice stating that her Sensitive Information was compromised in the Data Breach.

14. Defendant, Omni, is a California Nonprofit corporation, with its principal place of business at 4900 California Avenue Suite 400B Bakersfield, California 93309.

JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class. At least one class member and Defendant are citizens of different states.

16. This Court has personal jurisdiction over Defendant because Defendant maintains its principal place of business in this District and does substantial business in this District.

17. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claim occurred in this District.

STATEMENT OF FACTS

Omni

18. Omni is a Bakersfield, California company that offers "national award-winning network of state-of-the-art community health centers[.]"[1] Omni boasts a total annual revenue of $23.3 million.[2]

19. As part of its business, Omni receives and maintains the Sensitive Information of thousands of current and former patients. In doing so, Omni implicitly promises to safeguard their Sensitive Information.

[1] Omni, linkedin, https://www.linkedin.com/company/omni-family-health/ (last visited October 19, 2024).
[2] Zoominfo, Omni, https://omnifamilyhealth.org/policies/notice-of-privacy-practices/#:~:text=Your%20Health%20Information%20Rights,a%20reasonable%2C%20cost%2Dbased%20fee (last visited October 19, 2024).

20. In collecting and maintaining its current and former patients' Sensitive Information, Omni agreed it would safeguard the data in accordance with state law, and federal law. After all, Plaintiff and Class Members themselves took reasonable steps to secure their Sensitive Information

21. Indeed, Defendant boasts in its Privacy Policy that it "is required to [] by law maintain the privacy and security of your protected health information." Defendant further assures its patients that it "will let you know promptly if a breach occurs that may have compromised the privacy or security of your information[.]"[3]

22. Despite recognizing its duty to do so, on information and belief, Omni has not implemented reasonable cybersecurity safeguards or policies to protect its patients' Sensitive Information or supervised its IT or data security agents and employees to prevent, detect, and stop breaches of its systems. As a result, Omni leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to patients' Sensitive Information.

The Data Breach

23. Plaintiff is an Omni patient. As a condition of treatment with Omni, Plaintiff provided Omni with her Sensitive Information. Omni used that Sensitive Information to facilitate its treatment of Plaintiff and required Plaintiff to provide that Sensitive Information to obtain treatment and care.

24. On information and belief, Defendant collects and maintains patients' Sensitive Information in its computer systems.

25. In collecting and maintaining Sensitive Information, Defendant implicitly agrees that it will safeguard the data using reasonable means according to state and federal law.

26. According to its Breach Notice, on August 7, 2024, Defendant was alerted to "claims that information was taken from our systems ***and posted on the dark web***." Ex. A

[3] Privacy Policy, Omni, https://omnifamilyhealth.org/policies/notice-of-privacy-practices/#:~:text=Your%20Health%20Information%20Rights,a%20reasonable%2C%20cost%2Dbased%20fee (last visited October 19, 2024).

(emphasis added). Following an internal investigation, Defendant confirmed that "the data posted on the dark web appeared to be ***related to Omni's patients and employees***." *Id*. (emphasis added).

27. In other words, Defendant's cyber and data security systems were so completely inadequate that it not only allowed cybercriminals to obtain files containing a treasure trove of thousands of its patients' highly private Sensitive Information, but it did not detect the Data Breach until the cybercriminals began posting or began threatening to post this Sensitive Information on the dark web.

28. Through its inadequate security practices, Defendant exposed Plaintiff's and the Class's Sensitive Information for theft and sale on the dark web.

29. Upon information and belief, the notorious ransomware gang, 'Hunters International ransomware group' was responsible for the cyberattack. Known as one of the most notorious and active ransomware actors, Hunters has perpetrated multiple high-profile breaches in the last year alone.[4] Defendant knew or should have known of the tactics that groups like Hunters employ.

30. With the Sensitive Information secured and stolen by Hunters International ransomware group, the hackers then purportedly issued a ransom demand to Defendant. Though Defendant has provided no public information on the ransom demand or payment, on information and belief, Hunters began releasing all 2.7 terabyte of files for download on August 7, 2024, and intends to release all stolen information on the dark web for access by cybercriminals following the deadline of its ransom demand.

[4] Quorum Cyber, https://www.quorumcyber.com/malware-reports/hunters-international-ransomware-report/ (last visited October 19, 2024).


FalconFeeds.io
@FalconFeedsio
HUNTERS INTERNATIONAL Ransomware Alert
Omni Family Health
Omni Family Health is a network of health centers in California's Central Valley, providing comprehensive medical, dental, and behavioral health services, has fallen victim to Hunters International ransomware. The group claims to have access to 2.7 TB of the organization's data and states that it will be published within the next 1 - 2 days.
#USA
#HuntersInternational #Ransomware #CyberAttack #DataBreach
#Infosec #DarkWeb
Omni Family Health
1d 03h 18m
United States of America
Revenue
$23.3M
Employees
113
Disclosures
0/8
2:52 pm · 6 Aug 2024 · 2,069 Views


Omni Family Health
1d 03h 21m
United States of America
Revenue
$23.3M
Employees
113
Disclosures
0/8
Omni
Family Health
Disclosures
HR
Awaiting
1d 03h 21m
Human resources, employees, reviews
View 102.8 GB · 141,969 files
Accounting
Upcoming
Contracts, Incomes, Reports, Tax, Federal grants, Invoices, corporation docs
View 1.6 TB · 1,059,063 files
Medical
Upcoming
Medical, insurances and health care
View 17.9 GB · 32,890 files
Employee data
Upcoming
network users data
SQL
Upcoming
databases
View 135.5 GB · 368,359 files
Insurance
Upcoming
View 3.4 GB · 6,042 files
Government
Upcoming
Government and Responsibilities
View 3.1 GB · 1,141 files
All Data
Upcoming
View 2.7 TB · 2,914,900 files

31. On or around October 11, 2024—two months after the Breach was finally discovered—Omni finally notified some Class Members about the Data Breach. However, notification is ongoing with many Class Members, including Plaintiff still awaiting formal notice.

32. Despite its duties and alleged commitments to safeguard Sensitive Information, Defendant did not in fact follow industry standard practices in securing patients' Sensitive Information, as evidenced by the Data Breach.

33. Usually in response to the Data Breach, a company will at least briefly outline how it intends to enhance the security of its systems to ensure no such event occurs again in the future. Not Defendant. Instead, Defendant places the onus on Plaintiff, merely telling Plaintiff that "cybersecurity is an ongoing concern for everyone" and "individuals can better protect themselves by taking [certain] steps [as outlined in the Breach Notice]". Ex. A.

34. Through its Breach Notice, Defendant also recognized the actual imminent harm and injury that flowed from the Data Breach, so it encouraged breach victims to be "remain vigilant by regularly reviewing your accounts and monitoring credit reports for suspicious activity." Ex. A.

35. Defendant also recognized through its Breach Notice, its duty to implement safeguards in accordance with state law, and federal law, insisting that, despite the Breach showing otherwise, "[t]he confidentiality, privacy, and security of information maintained by Omni remains our top priority." Ex. A.

36. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff's and the Class's Sensitive Information. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff's and the Class's financial accounts.

37. On information and belief, Omni has offered several months of complimentary credit monitoring services to victims, which does not adequately address the lifelong harm that

victims will face following the Data Breach. Indeed, the breach involves Sensitive Information that cannot be changed, such as Social Security numbers.

38. Even with several months' worth of credit monitoring services, the risk of identity theft and unauthorized use of Plaintiff's and Class Members' Sensitive Information is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

39. On information and belief, Defendant failed to adequately train and supervise its IT and data security agents and employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over its patients' Sensitive Information. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the Sensitive Information.

The Data Breach was a Foreseeable Risk of which Defendant was on Notice.

40. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare and healthcare adjacent industry preceding the date of the breach.

41. In light of recent high profile data breaches at other healthcare and healthcare adjacent companies, Defendant knew or should have known that its electronic records and patients' Sensitive Information would be targeted by cybercriminals.

42. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[5] The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[6]

[5] 2021 Data Breach Annual Report, ITRC, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf (last visited January 10, 2024).

[6] *Id*.

43. Indeed, cyberattacks against the healthcare industry have become increasingly common for over ten years, with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime." [7]

44. Cyberattacks on medical systems and healthcare and healthcare adjacent companies like Defendant have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[8]

45. In fact, many high-profile ransomware attacks have occurred in healthcare and healthcare adjacent companies, with an estimated that nearly half of all ransomware attacks being carried out are on healthcare companies, and with 85% of those attacks being ransomware similar to the one occurring here.[9]

46. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

Plaintiff's Experience

47. Plaintiff is an Omni patient and Data Breach victim. Indeed, on August 7, 2024, Plaintiff attempted to access her patient portal but discovered her patient portal and information relating to her portal access had been completely wiped. On information and belief, this was a result of the Breach.

48. Plaintiff is an Omni patient. As a condition of treatment with Omni, Plaintiff provided Omni with her Sensitive Information. Omni used that Sensitive Information to facilitate

---

[7] Gordon M. Snow Statement, FBI https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector (last visited January 10, 2024).

[8] Secret Service Warn of Targeted, Law360, https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited January 10, 2024).

[9] Ransomware explained, CSO, https://www.csoonline.com/article/563507/what-is-ransomware-how-it-works-and-how-to-remove-it.html (last visited January 10, 2024);

its treatment of Plaintiff and required Plaintiff to provide that Sensitive Information to obtain treatment and care.

49. Plaintiff provided her Sensitive Information to Defendant and trusted that it would use reasonable measures to protect it according to state and federal law.

50. Defendant deprived Plaintiff of the earliest opportunity to guard herself against the Data Breach's effects by completely failing to notify her in a prompt manner.

51. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff's Sensitive Information for theft by cybercriminals and sale on the dark web.

52. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

53. Plaintiff has and will spend considerable time and effort monitoring her accounts to protect herself from additional identity theft. Plaintiff fears for her personal financial security and uncertainty over what Sensitive Information was exposed in the Data Breach.

54. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

55. Plaintiff has suffered actual injury in the form of damages to and diminution in the value of their Sensitive Information—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

56. Plaintiff suffered actual injury from the exposure of her Sensitive Information — which violates her rights to privacy.

57. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Sensitive Information being placed in the hands of unauthorized third parties and possibly criminals.

58. Indeed, shortly after the Data Breach, Plaintiff began suffering a significant increase in medical related spam calls and emails. These spam calls suggests that her Sensitive Information is now in the hands of cybercriminals.

59. Once an individual's Sensitive Information is for sale and access on the dark web, as Plaintiff's PII is here as a result of the Breach, cybercriminals are able to use the stolen and compromised to gather and steal even more information.[10] On information and belief, Plaintiff's phone number and email address was compromised as a result of the Data Breach.

60. Plaintiff has a continuing interest in ensuring that her Sensitive Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

61. Plaintiff and members of the proposed Class have suffered injury from the misuse of their Sensitive Information that can be directly traced to Defendant.

62. As a result of Defendant's failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their Sensitive Information is used;

b. The diminution in value of their Sensitive Information;

c. The compromise and continuing publication of their Sensitive Information;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

[10] What do Hackers do with Stolen Information, Aura, https://www.aura.com/learn/what-do-hackers-do-with-stolen-information (last visited January 9, 2024).

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen Sensitive Information; and

h. The continued risk to their Sensitive Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the Sensitive Information in its possession.

63. Stolen Sensitive Information is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII alone can be worth up to $1,000.00 depending on the type of information obtained.

64. The value of Plaintiff's and the Class's Sensitive Information on the black market is considerable. Stolen Sensitive Information trades on the black market for years, and criminals frequently post stolen Sensitive Information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

65. It can take victims years to spot identity theft, giving criminals plenty of time to use that information for cash.

66. One such example of criminals using Sensitive Information for profit is the development of "Fullz" packages.

67. Cyber-criminals can cross-reference two sources of Sensitive Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

68. The development of "Fullz" packages means that stolen Sensitive Information from the Data Breach can easily be used to link and identify it to Plaintiff and the proposed Class' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Sensitive Information stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and

members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and the Class's stolen Sensitive Information is being misused, and that such misuse is fairly traceable to the Data Breach.

69. Defendant disclosed the Sensitive Information of Plaintiff and the Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the Sensitive Information of Plaintiff and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen Sensitive Information.

70. Defendant's failure to properly notify Plaintiff and members of the Class of the Data Breach exacerbated Plaintiff's and the Class's injury by depriving them of the earliest ability to take appropriate measures to protect their Sensitive Information and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendant failed to adhere to FTC guidelines.

71. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of Sensitive Information.

72. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the sensitive consumer information that it keeps;

b. properly dispose of Sensitive Information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

73. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

74. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

75. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

76. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' Sensitive Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Violated HIPAA

77. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information. [11]

[11] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, inter alia: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

78. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII and PHI is properly maintained.[12]

79. The Data Breach itself resulted from a combination of inadequacies showing Defendant's failure to comply with safeguards mandated by HIPAA. Defendant's security failures include, but are not limited to:

a. Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);

b. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

c. Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

d. Failing to ensure compliance with HIPAA security standards by Defendant in violation of 45 C.F.R. § 164.306(a)(4);

e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

[12] *See* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

h. Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

80. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations.

Defendant Fails to Comply with Industry Standards

81. As noted above, experts studying cyber security routinely identify entities in possession of PII and PHI as being particularly vulnerable to cyberattacks because of the value of the Sensitive Information which they collect and maintain.

82. Several best practices have been identified that a minimum should be implemented by employers in possession of PII and PHI, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

83. Other best cybersecurity practices that are standard for employers include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

84. Upon information and belief, Defendants failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both

the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04).

85. These foregoing frameworks are existing and applicable industry standards for an employer's obligations to provide adequate data security for its employees. Upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

CLASS ACTION ALLEGATIONS

86. Plaintiff is suing on behalf of herself and the proposed Class ("Class"), defined as follows:

> All individuals residing in the United States whose Sensitive Information was compromised in the Data Breach, including all those who received notice of the breach.

87. Excluded from the Class is Defendant, their agents, affiliates, parents, subsidiaries, any entity in which Defendant have a controlling interest, any of Defendant's officers or directors, any successors, and any Judge who adjudicates this case, including their staff and immediate family.

88. Plaintiff reserves the right to amend the class definition.

89. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

a. **Numerosity**. Plaintiff is representative of the Class, consisting of several 470,000 of members, far too many to join in a single action;

b. **Ascertainability**. Members of the Class are readily identifiable from information in Defendant's possession, custody, and control;

c. **Typicality**. Plaintiff's claims are typical of class claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's interests. Her interests do not conflict with the Class's interests, and she has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Commonality**. Plaintiff's and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for the Class. Indeed, it will be necessary to answer the following questions:

i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's Sensitive Information;

ii. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

iii. Whether Defendant were negligent in maintaining, protecting, and securing Sensitive Information;

iv. Whether Defendant breached contract promises to safeguard Plaintiff's and the Class's Sensitive Information;

v. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

vi. Whether Defendant's Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiff's and the Class's injuries;

viii. What the proper damages measure is; and

ix. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

90. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

91. Plaintiff realleges all previous paragraphs as if fully set forth below.

92. Plaintiff and members of the Class entrusted their Sensitive Information to Defendant. Defendant owed to Plaintiff and the Class a duty to exercise reasonable care in handling and using the Sensitive Information in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

93. Defendant owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard their Sensitive Information in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that Sensitive Information —just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and the Class's Sensitive Information by disclosing and providing access to this information to unauthorized third parties and by failing to properly supervise both the way the Sensitive Information was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

94. Defendant owed to Plaintiff and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their Sensitive Information. Defendant also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and the Class to take appropriate measures to protect their Sensitive Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

95. Defendant owed these duties to Plaintiff and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant

knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff's and the Class's Sensitive Information.

96. The risk that unauthorized persons would attempt to gain access to the Sensitive Information and misuse it was foreseeable. Given that Defendant holds vast amounts of Sensitive Information, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the Sensitive Information —whether by malware or otherwise.

97. Sensitive Information is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Sensitive Information of Plaintiff and the Class and the importance of exercising reasonable care in handling it.

98. Defendant breached its duties by failing to exercise reasonable care in supervising its employees, agents, contractors, vendors, and suppliers, and in handling and securing the Sensitive Information of Plaintiff and the Class which actually and proximately caused the Data Breach and Plaintiff's and the Class's injury. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's and members of the Class's injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

99. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their Sensitive Information by criminals, improper disclosure of their Sensitive Information, lost benefit of their bargain, lost value of their Sensitive Information, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's

negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face. .

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

100. Plaintiff realleges all previous paragraphs as if fully set forth below.

101. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and the Class's Sensitive Information.

102. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers or, in this case, patients' Sensitive Information. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and the members of the Class's Sensitive Information.

103. Defendant breached its duties to Plaintiff and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Sensitive Information.

104. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach.

105. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the

healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

106. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Sensitive Information.

107. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and the Class's Sensitive Information and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Sensitive Information Defendant collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

108. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

109. Defendant violated its duty under HIPAA by failing to use reasonable measures to protect their PHI and by not complying with applicable regulations detailed supra. Here too, Defendant's conduct was particularly unreasonable given the nature and amount of Sensitive Information Defendant collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

110. But for Defendant's wrongful and negligent breach of the duties owed to Plaintiff and members of the Class, Plaintiff and members of the Class would not have been injured.

111. The injury and harm suffered by Plaintiff and members of the Class were the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties and that its breach would cause Plaintiff and members

of the Class to suffer the foreseeable harms associated with the exposure of their Sensitive Information.

112. Had Plaintiff and the Class known that Defendant did not adequately protect their Sensitive Information, Plaintiff and members of the Class would not have entrusted Defendant with their Sensitive Information.

113. Defendant's various violations and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

114. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of Sensitive Information; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Sensitive Information, entitling them to damages in an amount to be proven at trial.

115. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class members have suffered and will suffer the continued risks of exposure of their Sensitive Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect their Sensitive Information in its continued possession.

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

116. Plaintiff realleges all previous paragraphs as if fully set forth below.

117. Plaintiff and the Class delivered their Sensitive Information to Defendant as part of the process of obtaining treatment and services provided by Defendant.

118. Plaintiff and Class Members entered into implied contracts with Defendant under which Defendant agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class Members if and when their data had been breached and compromised.

Each such contractual relationship imposed on Defendant an implied covenant of good faith and fair dealing by which Defendant was required to perform its obligations and manage Plaintiff's and Class Members' data in a manner which comported with the reasonable expectations of privacy and protection attendant to entrusting such data to Defendant.

119. In providing their Sensitive Information, Plaintiff and Class Members entered into an implied contract with Defendant whereby Defendant, in receiving such data, became obligated to reasonably safeguard Plaintiff's and the other Class Members' Sensitive Information.

120. In delivering their Sensitive Information to Defendant, Plaintiff and Class Members intended and understood that Defendant would adequately safeguard that data.

121. Plaintiff and the Class Members would not have entrusted their Sensitive Information to Defendant in the absence of such an implied contract.

122. Defendant accepted possession of Plaintiff's and Class Members' Sensitive Information.

123. Had Defendant disclosed to Plaintiff and Class Members that Defendant did not have adequate computer systems and security practices to secure patients' Sensitive Information, Plaintiff and members of the Class would not have provided their Sensitive Information to Defendant.

124. Defendant recognized that patients' Sensitive Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and Class Members.

125. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

126. Defendant breached the implied contract with Plaintiff and Class Members by failing to take reasonable measures to safeguard its data.

127. Defendant breached the implied contract with Plaintiff and Class Members by failing to promptly notify them of the access to and exfiltration of their Sensitive Information.

128. As a direct and proximate result of the breach of the contractual duties, Plaintiff and Class Members have suffered actual, concrete, and imminent injuries. The injuries suffered by Plaintiff and the Class Members include: (a) the invasion of privacy; (b) the compromise, disclosure, theft, and unauthorized use of their Sensitive Information; (c) economic costs associated with the time spent to detect and prevent identity theft, including loss of productivity; (d) monetary costs associated with the detection and prevention of identity theft; (e) economic costs, including time and money, related to incidents of actual identity theft; (f) the emotional distress, fear, anxiety, nuisance and annoyance of dealing related to the theft and compromise of their Sensitive Information; (g) the diminution in the value of the services bargained for as Plaintiff and Class Members were deprived of the data protection and security that Defendant promised when Plaintiff and the proposed class entrusted Defendant with their Sensitive Information; and (h) the continued and substantial risk to Plaintiff's and Class Members' Sensitive Information, which remains in the Defendant's possession with inadequate measures to protect Plaintiff's and Class Members' Sensitive Information.

COUNT IV
Breach of the Implied Covenant of Good Faith and Fair Dealing
(On Behalf of Plaintiff and the Class)

129. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

130. Under California law, every contract imposes on each party a duty of good faith and fair dealing in each performance and its enforcement. Thus, parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—and not merely the letter—of the bargain. In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

131. Subterfuge and evasion violate the duty of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or consist of inaction. And fair dealing may require more than honesty.

132. Here, Plaintiff and Defendant entered into a contract (implied in law, fact, or otherwise) whereby Defendant agreed to:

a. use a portion of the funds paid by Plaintiff and Class Members to pay for adequate cybersecurity measures;

b. use adequate cybersecurity measures as required by state law, federal law, and Defendant's contractual agreements (implied or otherwise); and

c. notify them promptly of any exposure of their Sensitive Information.

133. As current and former employees, Plaintiff and Class Members fully fulfilled their contractual obligations when they provided their labor to Defendant.

134. Furthermore, the conditions precedent (if any) to Defendant's performance have already occurred.

135. Defendant unfairly interfered with the Plaintiff's and Class Members' rights to receive the benefits of the contract—and breached the covenant of good faith and fair dealing—by, *inter alia*:

a. failing to safeguard their information;

b. failing to notify them promptly of the intrusion into its computer systems that compromised such information.

c. failing to comply with industry standards;

d. failing to comply with its legal obligations; and

e. failing to ensure the confidentiality and integrity of the electronic Sensitive Information that Defendant created, received, maintained, and transmitted.

136. Defendant's material breaches were the direct and proximate cause of Plaintiff's and Class Members' injuries (as detailed *supra*).

COUNT V
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

137. Plaintiff realleges all previous paragraphs as if fully set forth below.

138. This claim is pleaded in the alternative to the breach of implied contractual duty claim.

139. Plaintiff and members of the Class conferred a benefit upon Defendant in providing Sensitive Information to Defendant.

140. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiff and the Class. Defendant also benefited from the receipt of Plaintiff's and the Class's Sensitive Information, as this was used to facilitate the treatment, services, and goods it sold to Plaintiff and the Class.

141. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff and the Class's Sensitive Information because Defendant failed to adequately protect their Sensitive Information. Plaintiff and the proposed Class would not have provided their Sensitive Information to Defendant had they known Defendant would not adequately protect their Sensitive Information.

142. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and members of the Class all unlawful or inequitable proceeds received by them because of their misconduct and Data Breach.

COUNT VI
Invasion of Privacy
Cal. Const. ART. 1 § 1
(On Behalf of Plaintiff and the Class)

143. Plaintiff realleges all previous paragraphs as if fully set forth below.

144. Plaintiff and Class Members had a reasonable expectation of privacy in their communications with Defendant via its communications platforms and services therein.

145. Plaintiff and Class Members communicated Sensitive Information that they intended for only Defendant to receive and that they understood Defendant would keep private.

146. Defendant's disclosure of the substance and nature of those communications to third parties without the knowledge and consent of Plaintiff and Class Members is an intentional intrusion on Plaintiff's and Class Members' solitude or seclusion and their private affairs and concerns.

147. Plaintiff and Class Members had a reasonable expectation of privacy given Defendant's representations, Privacy Policies and HIPAA. Moreover, Plaintiff and Class Members have a general expectation that their communications regarding healthcare with their healthcare providers will be kept confidential. Defendant's disclosure of Plaintiff's and the Class's PHI coupled with Sensitive Information is highly offensive to the reasonable person.

148. As a result of Defendant's actions, Plaintiff and Class Members have suffered harm and injury, including but not limited to invasion of their privacy rights, the unauthorized access of their Sensitive Information by third parties, improper disclosure of their Sensitive Information, lost benefit of their bargain, lost value of their Sensitive Information, and lost time and money incurred to mitigate and remediate the effects of use of their information that resulted from and were caused by Defendant's conduct. These injuries are ongoing, imminent, immediate, and continuing.

149. Plaintiff and Class Members have been damaged as a direct and proximate result of Defendant's invasion of their privacy and are entitled to just compensation, including monetary damages.

150. Plaintiff and Class Members seek appropriate relief for that injury, including but not limited to actual and compensatory damages, and all other relief they may be entitled to reasonably compensate Plaintiff and Class Members for the harm to their privacy interests as a result of its intrusions upon Plaintiff's and Class Members' privacy.

151. Plaintiff also seek such other relief as the Court may deem just and proper.

COUNT VII
Violation of California's Unfair Competition Law ("UCL")
Cal Bus. & Prof. Code § 17200, *et seq*.
(On Behalf of Plaintiff and the Class)

152. Plaintiff realleges all previous paragraphs as if fully set forth below.

153. Defendant engaged in unlawful and unfair business practices in violation of Cal. Bus. & Prof. Code § 17200, *et seq*. which prohibits unlawful, unfair, or fraudulent business acts or practices ("UCL").

154. Defendant's conduct is unlawful because it violates the California Consumer Privacy Act of 2018, Civ. Code § 1798.100, et seq. (the "CCPA"), and other state data security laws.

155. Defendant stored the Sensitive Information of Plaintiff and the Class in its computer systems and knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied with applicable regulations and that would have kept Plaintiff's and the Class's Sensitive Information secure so as to prevent the loss or misuse of that Sensitive Information.

156. Defendant failed to disclose to Plaintiff and the Class that their Sensitive Information was not secure. However, Plaintiff and the Class were entitled to assume, and did assume, that Defendant had secured their Sensitive Information. At no time were Plaintiff and the Class on notice that their Sensitive Information was not secure, which Defendant had a duty to disclose.

157. Defendant also violated California Civil Code § 1798.150 by failing to implement and maintain reasonable security procedures and practices, resulting in an unauthorized access and exfiltration, theft, or disclosure of Plaintiff's and the Class's nonencrypted and nonredacted Sensitive Information.

158. Had Defendant complied with these requirements, Plaintiff and the Class would not have suffered the damages related to the data breach.

159. Defendant's conduct was unlawful, in that it violated the CCPA.

160. Defendant's acts, omissions, and misrepresentations as alleged herein were unlawful and in violation of, inter alia, Section 5(a) of the Federal Trade Commission Act.

161. Defendant's conduct was also unfair, in that it violated a clear legislative policy in favor of protecting consumers from data breaches.

162. Defendant's conduct is an unfair business practice under the UCL because it was immoral, unethical, oppressive, and unscrupulous and caused substantial harm. This conduct includes employing unreasonable and inadequate data security despite its business model of actively collecting Sensitive Information.

163. Defendant also engaged in unfair business practices under the "tethering test." Its actions and omissions, as described above, violated fundamental public policies expressed by the California Legislature. See, e.g., Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern."). Defendant's acts and omissions thus amount to a violation of the law.

164. Instead, Defendant made the Sensitive Information of Plaintiff and the Class accessible to scammers, identity thieves, and other malicious actors, subjecting Plaintiff and the Class to an impending risk of identity theft. Additionally, Defendant's conduct was unfair under the UCL because it violated the policies underlying the laws set out in the prior paragraph.

165. As a result of those unlawful and unfair business practices, Plaintiff and the Class suffered an injury-in-fact and have lost money or property.

166. The injuries to Plaintiff and the Class greatly outweigh any alleged countervailing benefit to consumers or competition under all of the circumstances.

167. There were reasonably available alternatives to further Defendant's legitimate business interests, other than the misconduct alleged in this complaint.

168. Therefore, Plaintiff and the Class are entitled to equitable relief, including restitution of all monies paid to or received by Defendant; disgorgement of all profits accruing to Defendant because of its unfair and improper business practices; a permanent injunction enjoining Defendant's unlawful and unfair business activities; and any other equitable relief the Court deems proper.

COUNT VIII
Violation of the California Consumer Privacy Act
Cal. Civ. Code § 1798.150
(On Behalf of Plaintiff and the Class)

169. Plaintiff realleges all previous paragraphs as if fully set forth below.

170. Defendant violated California Civil Code § 1798.150 of the CCPA by failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the nonencrypted Sensitive Information of Plaintiff and the Class. As a direct and proximate result, Plaintiff's, and the Class's nonencrypted and nonredacted Sensitive Information was subject to unauthorized access and exfiltration, theft, or disclosure.

171. Defendant is a business organized for the profit and financial benefit of its owners according to California Civil Code § 1798.140, that collects the personal information of its customers, and whose annual gross revenues exceed the threshold established by California Civil Code § 1798.140(d).

172. Plaintiff and Class Members seek injunctive or other equitable relief to ensure Defendant hereinafter adequately safeguards Sensitive Information by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold Sensitive Information, including Plaintiff's and Class members' Sensitive Information. Plaintiff and Class members have an interest in ensuring that their Sensitive Information is reasonably protected, and Defendant has demonstrated a pattern of failing to adequately safeguard this information.

173. Pursuant to California Civil Code § 1798.150(b), Plaintiff mailed a CCPA notice letter to Defendant's registered service agents, detailing the specific provisions of the CCPA that Defendant has violated and continues to violate. If Defendant cannot cure within 30 days—and Plaintiff believes such cure is not possible under these facts and circumstances—then Plaintiff intends to promptly amend this Complaint to seek statutory damages as permitted by the CCPA.

174. As described herein, an actual controversy has arisen and now exists as to whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of the information so as to protect the personal information under the CCPA.

175. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by Defendant.

COUNT IX
Violation of the California Customer Records Act
Cal. Civ. Code § 1798.80, *et seq*.
(On Behalf of Plaintiff and the Class)

176. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

177. Under the California Customer Records Act, any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" must "disclose any breach of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82. The disclosure must "be made in the most expedient time possible and without unreasonable delay" but disclosure must occur "immediately following discovery [of the breach], if the personal information was, ***or*** is reasonably believed to have been, acquired by an unauthorized person." *Id* (emphasis added).

178. The Data Breach constitutes a "breach of the security system" of Defendant.

179. An unauthorized person acquired the personal, unencrypted information of Plaintiff and the Class.

180. Defendant knew that an unauthorized person had acquired the personal, unencrypted information of Plaintiff and the Class but waited approximately two months to notify them. Given the severity of the Data Breach, two months was an unreasonable delay.

181. Defendant's unreasonable delay prevented Plaintiff and the Class from taking appropriate measures from protecting themselves against harm.

182. Because Plaintiff and the Class were unable to protect themselves, they suffered incrementally increased damages that they would not have suffered with timelier notice.

183. Plaintiff and the Class are entitled to equitable relief and damages in an amount to be determined at trial.

COUNT X
Violation of the California Confidentiality of Medical Information Act
Cal. Civ. Code § 56, *et seq*.
(On Behalf of Plaintiff and the Class)

184. Plaintiff realleges all previous paragraphs as if fully set forth below.

185. Defendant is "a provider of health care," as defined in Cal. Civ. Code §56.05(m) and is therefore subject to the requirements of the CMIA, Cal. Civ. Code §56.10(a), (d) and (e), 56.36(b), 56.101(a) and (b).

186. At all relevant times, Defendant was a health care provider because they had the "purpose of maintaining medical information to make the information available to the individual or to a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manager his or her information, or for the diagnosis or treatment of the individual."

187. As a provider of health care or a contractor, Defendant is required by the CMIA to ensure that medical information regarding patients is not disclosed or disseminated and/or released without patient's authorization, and to protect and preserve the confidentiality of the medical

information regarding a patient, under Civil Code §§ 56.06, 56.10, 56.13, 56.20, 56.245, 56.26, 56.35, 56.36, and 56.101.

188. As a provider of health care or a contractor, Defendant is required by the CMIA not to disclose medical information regarding a patient without first obtaining an authorization under Civil Code §§ 56.06, 56.10, 56.13, 56.20, 56.245, 56.26, 56.35, and 56.104.

189. Defendant is a person/entity licensed under California under California's Business and Professions Code, Division 2. See Cal. Bus. Prof. Code § 4000, *et seq*.

190. Plaintiff and Class Members are "patients" as defined in CMIA, Cal. Civ. Code §56.05(k) ("'Patient' means any natural person, whether or not still living, who received health care services from a provider of health care and to whom medical information pertains."). Furthermore, Plaintiff and Class Members, as patients and customers of Defendant, had their individually identifiable "medical information," within the meaning of Civil Code § 56.05(j), created, maintained, preserved, and stored on Defendant's computer network, and were patients on or before the date of the Data Breach.

191. Defendant disclosed "medical information," as defined in CMIA, Cal. Civ. Code § 56.05(j), to unauthorized persons without first obtaining consent, in violation of Cal. Civ. Code § 56.10(a). The disclosure of information to unauthorized individuals in the Data Breach resulted from the affirmative actions of Defendant's employees, which allowed the hackers to see and obtain Plaintiff's and Class Members' medical and Sensitive Information.

192. Defendant negligently created, maintained, preserved, stored, and then exposed Plaintiff's and Class Members' individually identifiable "medical information," within the meaning of Cal. Civ. Code § 56.05(j), including Plaintiff's and California Class members' names, addresses, medical information, and health insurance information, that alone or in combination with other publicly available information, reveals their identities. Specifically, Defendant knowingly allowed and affirmatively acted in a manner that allowed unauthorized parties to access, exfiltrate, and actually view Plaintiff's and Class Members' confidential Sensitive Information.

193. Defendant's negligence resulted in the release of individually identifiable medical information pertaining to Plaintiff and Class Members to unauthorized persons and the breach of the confidentiality of that information. Defendant's negligent failure to maintain, preserve, store, abandon, destroy, and/or dispose of Plaintiff's and Class Members' medical information in a manner that preserved the confidentiality of the information contained therein, in violation of Cal. Civ. Code §§ 56.06 and 56.101(a).

194. Defendant also violated Sections 56.06 and 56.101 of the CMIA, which prohibit the negligent creation, maintenance, preservation, storage, abandonment, destruction, or disposal of confidential personal medical information.

195. Plaintiff's and Class Members' medical information was accessed and actually viewed by hackers in the Data Breach.

196. Plaintiff's and Class Members' medical information that was the subject of the Data Breach included "electronic medical records" or "electronic health records" as referenced by Civil Code § 56.101(c) and defined by 42 U.S.C. § 17921(5).

197. Defendant's computer systems did not protect and preserve the integrity of electronic medical information in violation of Cal. Civ. Code § 56.101(b)(1)(A). As a direct and proximate result of Defendant's above-noted wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, and violation of the CMIA, Plaintiff and the Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, inter alia:

a. present, imminent, immediate and continuing increased risk of identity theft, identity fraud and medical fraud –risks justifying expenditures for protective and remedial services for which they are entitled to compensation;

b. invasion of privacy;

c. breach of the confidentiality of the PHI;

d. statutory damages under the California CMIA;

e. deprivation of the value of their PHI, for which there is well-established national and international markets; and/or,

f. the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

198. As a direct and proximate result of Defendant's wrongful actions, inaction, omission, and want of ordinary care that directly and proximately caused the release of Plaintiff's and Class Members' Sensitive Information, Plaintiff and Class Members' personal medical information was viewed by, released to, and disclosed to third parties without Plaintiff's and Class Members' written authorization.

199. Defendant's negligent failure to maintain, preserve, store, abandon, destroy, and/or dispose of Plaintiff's and Class Members' medical information in a manner that preserved the confidentiality of the information contained therein violated the CMIA.

200. Plaintiff and the Class Members were injured and have suffered damages, as described above, from Defendant's illegal and unauthorized disclosure and negligent release of their medical information in violation of Cal. Civ. Code §§56.10 and 56.101, and therefore seek relief under Civ. Code §§ 56.35 and 56.36, which allows for actual damages, nominal statutory damages of $1,000, punitive damages of $3,000, injunctive relief, and attorneys' fees, expenses and costs.

COUNT XI
Declaratory Judgment
(On Behalf of Plaintiff and the Class)

201. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

202. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. The Court has broad authority to restrain acts, such as those alleged herein, which are tortious and unlawful.

203. In the fallout of the Data Breach, an actual controversy has arisen about Defendant's various duties to use reasonable data security. On information and belief, Plaintiff alleges that Defendant's actions were—and *still* are—inadequate and unreasonable. And Plaintiff and Class Members continue to suffer injury from the ongoing threat of fraud and identity theft.

204. Given its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owed—and continues to owe—a legal duty to use reasonable data security to secure the data entrusted to it;

b. Defendant has a duty to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

c. Defendant breached, and continues to breach, its duties by failing to use reasonable measures to the data entrusted to it; and

d. Defendant breaches of its duties caused—and continues to cause—injuries to Plaintiff and Class Members.

205. The Court should also issue corresponding injunctive relief requiring Defendant to use adequate security consistent with industry standards to protect the data entrusted to it.

206. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy if Defendant experiences a second data breach.

207. And if a second breach occurs, Plaintiff and the Class will lack an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages—while warranted for out-of-pocket damages and other legally quantifiable and provable damages—cannot cover the full extent of Plaintiff and Class Members' injuries.

208. If an injunction is not issued, the resulting hardship to Plaintiff and Class Members far exceeds the minimal hardship that Defendant could experience if an injunction is issued.

209. An injunction would benefit the public by preventing another data breach—thus preventing further injuries to Plaintiff, Class Members, and the public at large.

PRAYER FOR RELIEF

Plaintiff and the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing her counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements Plaintiff the Data Breach and the stolen Sensitive Information;

E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

Plaintiff hereby demands that this matter be tried before a jury.

Dated: October 20, 2024

By: */s/ Andrew G. Gunem*

Andrew G. Gunem (SBN 354042)
STRAUSS BORRELLI PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, Illinois 60611
T: (872) 263-1100
F: (872) 263-1109
agunem@straussborrelli.com

Attorney for Plaintiff and the Proposed Class